Available online at www.sciencedirect.com

SCIENCE DIRECT®

Journal of Combinatorial Theory, Series A 113 (2006) 608–624

Journal of Combinatorial Theory Series A

www.elsevier.com/locate/jcta

New families of atomic Latin squares and perfect 1-factorisations

Darryn Bryant[a], Barbara Maenhaut[a], Ian M. Wanless[b,1]

[a] *Department of Mathematics, University of Queensland, Qld 4072, Australia*

[b] *School of Engineering and Logistics, Charles Darwin University, Darwin NT 0909, Australia*

Received 11 August 2004

Communicated by William Kantor

Available online 18 July 2005

Abstract

A perfect 1-factorisation of a graph G is a decomposition of G into edge disjoint 1-factors such that the union of any two of the factors is a Hamiltonian cycle. Let $p \geqslant 11$ be prime. We demonstrate the existence of two non-isomorphic perfect 1-factorisations of K_{p+1} (one of which is well known) and five non-isomorphic perfect 1-factorisations of $K_{p,p}$. If 2 is a primitive root modulo p, then we show the existence of 11 non-isomorphic perfect 1-factorisations of $K_{p,p}$ and 5 main classes of atomic Latin squares of order p. Only three of these main classes were previously known. One of the two new main classes has a trivial autotopy group.

Keywords: Perfect 1-factorisation; Atomic latin square; Totally symmetric; Hamiltonian cycle; Even starter; Autotopy group

1. Introduction

1.1. One-factorisations

A 1-*factorisation* of a graph is a partition of the edge-set of that graph into 1-factors (perfect matchings). A 1-factorisation is *perfect* if the union of any two of its 1-factors is a Hamiltonian cycle. For a background on these concepts, consult [13,14].

E-mail addresses: db@maths.uq.edu.au (D. Bryant), bmm@maths.uq.edu.au (B. Maenhaut), ian.wanless@cdu.edu.au (I.M. Wanless).

[1] Written while the third author was employed by the Department of Computer Science at the Australian National University.

0097-3165/$ - see front matter © 2005 Elsevier Inc. All rights reserved.
doi:10.1016/j.jcta.2005.05.003

A common construction method for 1-factorisations of complete graphs is the use of an even starter. Let G be an abelian group (written multiplicatively) of order $2n$ with identity e and a unique element g^* of order two. An *even starter* in G is a set $E = \{\{x_1, y_1\}, \{x_2, y_2\}, \ldots, \{x_{n-1}, y_{n-1}\}\}$ such that

(1) $x_1, y_1, x_2, y_2, \ldots, x_{n-1}, y_{n-1}$ are all the non-identity elements of G except one, denoted by m_E;
(2) $\{x_i^{-1}y_i, y_i^{-1}x_i : 1 \leqslant i \leqslant n-1\} = G \setminus \{e, g^*\}$.

An even starter E in G induces a 1-factorisation of K_{2n+2} as follows, see for instance [1]. Label the vertices of K_{2n+2} with the elements of G and two infinity elements, ∞_1 and ∞_2. Define $x\infty_1 = \infty_1$ and $x\infty_2 = \infty_2$ for all $x \in G$. Let

$$E^* = E \cup \{\{e, \infty_1\}, \{m_E, \infty_2\}\}$$

and

$$Q^* = \{\{x, xg^*\} : x \in G\} \cup \{\{\infty_1, \infty_2\}\}.$$

The 1-factorisation $\mathcal{F}_E$ of K_{2n+2} is then given by the translates of E^* and the 1-factor Q^*; that is, $\mathcal{F}_E = \{xE^* : x \in G\} \cup Q^*$, where $xE^* = \{\{xa, xb\} : \{a, b\} \in E^*\}$ for $x \in G$. For this 1-factorisation, the group G is known as the *starter group*.

We now define the automorphism group of a 1-factorisation $\mathcal{F}$ of K_{2n}. Let the 1-factors of $\mathcal{F}$ be $F_1, F_2, \ldots, F_{2n-1}$. If π is an element of S_{2n}, the full symmetric group on the vertices of K_{2n}, then define $\pi[F_i] = \{\{\pi(x), \pi(y)\} : \{x, y\} \in F_i\}$ and $\pi[\mathcal{F}] = \{\pi[F_i] : 1 \leqslant i \leqslant 2n-1\}$. We define the automorphism group of $\mathcal{F}$ by $\mathrm{Aut}(\mathcal{F}) = \{\pi : \pi \in S_{2n} \text{ and } \pi[\mathcal{F}] = \mathcal{F}\}$.

There is a well-known 1-factorisation of the complete graph K_{p+1}, often called the *patterned* 1-*factorisation* and denoted by GK_{p+1}. Label the vertices of K_{p+1} by $0, 1, \ldots, p-1, \infty$, and for each $i = 0, 1, \ldots, p-1$ define a 1-factor G_i as

$$G_i = \{\{i, \infty\}\} \cup \{\{x, y\} : x + y = 2i \bmod p\}.$$

Then $GK_{p+1} = \{G_i : 0 \leqslant i \leqslant p-1\}$.

It was shown in [2] that $|\mathrm{Aut}(GK_{p+1})| = p(p-1)$ and that $\mathrm{Aut}(GK_{p+1})$ is generated by the permutations ρ and π_r, where r is a primitive root modulo p,

$$\rho(i) = \begin{cases} (i+1) \bmod p, & i \neq \infty, \\ \infty, & i = \infty, \end{cases} \quad \text{and} \quad \pi_r(i) = \begin{cases} ri \bmod p, & i \neq \infty, \\ \infty, & i = \infty. \end{cases}$$

It is well known that GK_{p+1} is perfect when p is prime [14]. A major result of this paper is:

Theorem 1.1. *For each prime $p \geqslant 11$, there is a perfect* 1-*factorisation of K_{p+1} which is not isomorphic to GK_{p+1}.*

1.2. Latin squares

A *Latin square* of order n is an $n \times n$ matrix in which each row and column is a permutation of some (fixed) symbol set of size n. It is often convenient to have the rows, columns and

symbols indexed by a common set Σ, which we call the *index set*. The use of a common index set makes a number of the concepts defined below (such as conjugacy and isomorphism) much more natural than they would otherwise be. For most of this paper we use $\Sigma = \mathbb{Z}_p$, the integers modulo a prime p.

Suppose that L is a Latin square with index set Σ. We use $L_{i,j}$ to indicate the symbol in row i and column j of L. Then each row r of L defines a permutation $\sigma_r = \sigma_r(L)$ of Σ by $x \mapsto L_{r,x}$ for each $x \in \Sigma$. Moreover, each ordered pair (r, s) of rows of L defines a permutation $\sigma_{r,s} = \sigma_{r,s}(L)$ of Σ by $L_{r,x} \mapsto L_{s,x}$ for each $x \in \Sigma$. It is clear from these definitions that $\sigma_{r,s} = (\sigma_{s,r})^{-1}$ and $\sigma_{r,s} = \sigma_s \circ (\sigma_r)^{-1}$. For permutations such as the ones we have just defined, we will often find it convenient to consider the corresponding digraph. For any permutation π of the set Σ we let $D(\pi)$ denote the digraph with vertices Σ and a directed edge from x to $\pi(x)$ for each $x \in \Sigma$.

It is often useful to think of a Latin square of order n as a set of n^2 triples of the form (row, column, symbol). The Latin property means that distinct triples never agree in more than one coordinate. For a Latin square L, we will say that the triple $(i, j, L_{i,j})$ belongs to L and write $(i, j, L_{i,j}) \in L$. For each Latin square there are six *conjugate* squares obtained by (uniformly) permuting the coordinates of each triple. For example, the transpose of L is obtained by swapping the row and column coordinates in each triple. The *row-inverse* of L is obtained by swapping the column and symbol coordinates in each triple. This has the effect of replacing each σ_r by its inverse. A square that is equal to its row-inverse is said to be *involutory*, since in such a square each σ_r is an involution.

A Latin square L is *symmetric* if $(i, j, k) \in L$ implies $(j, i, k) \in L$, that is, L is equal to its transpose. A Latin square L is *totally symmetric* if when $(i, j, k) \in L$, then

$$\{(i,k,j),\ (j,i,k),\ (j,k,i),\ (k,i,j),\ (k,j,i)\} \subset L.$$

Thus, all six conjugates of a totally symmetric Latin square are equal.

A Latin subrectangle of a Latin square L is a rectangular submatrix of L in which the same symbols occur in each row. If R is a $2 \times \ell$ Latin subrectangle of L, and R is minimal in that it contains no $2 \times \ell'$ Latin subrectangle for $2 \leqslant \ell' < \ell$, then we say that R is a row cycle of length ℓ. Note that a row cycle of length ℓ between two rows r and s corresponds in a natural way to a cycle of length ℓ in the permutation $\sigma_{r,s}(L)$. Column cycles and symbol cycles can be defined similarly, and the operations of conjugacy on L interchange these objects.

A Latin square of order n is *row-Hamiltonian* if every row cycle has length n, symbol-Hamiltonian if every symbol cycle has length n, and column-Hamiltonian if every column cycle has length n. These three types of square are related by conjugacy. A Latin square is *atomic* if it is row-Hamiltonian, symbol-Hamiltonian and column-Hamiltonian. In other words, a square is atomic if all its conjugates are row-Hamiltonian. This terminology is based on [15], where the name "atomic Latin square" was coined, although that paper used pan-Hamiltonian for what we are calling row-Hamiltonian. Row-Hamiltonian Latin squares are studied in [4,15]. Atomic Latin squares have been studied in [11,12,17,18].

An *isotopy* of a Latin square L is a permutation of its rows, permutation of its columns and permutation of its symbols. The resulting square is said to be *isotopic* to L and the set of all squares isotopic to L is called an *isotopy class*. In the special case when the same permutation is applied to the rows, columns and symbols we say that the isotopy is an

isomorphism. An isotopy that maps L to itself is called an *autotopy* of L and any autotopy that is an isomorphism is called an *automorphism*. The *main class* of L is the set of squares which are isotopic to some conjugate of L. Latin squares belonging to the same main class are said to be *paratopic* and a map which combines an isotopy with conjugation is called a *paratopy*. A paratopy which maps a Latin square to itself is called an *autoparatopy* of the square.

A Latin square L of order n which has a cyclic automorphism of order $n - b$ is called a *B_b-type square*. See [16] for a survey article devoted to such squares, and [3] for existence results on B_b-type squares which have additional symmetry properties, such as being totally symmetric. It was found in [11] that four of the seven main classes of atomic Latin squares of order 11 contain strikingly similar B_1-type squares. We show in Section 4 that this observation is part of a general pattern. Indeed, our second major result of this paper is:

Theorem 1.2. *Let $p \geqslant 11$ be a prime for which 2 is a primitive root. There are at least five distinct main classes of atomic Latin squares of order p. Four of the main classes contain B_1-type squares, while squares in the fifth main class have trivial autotopy group.*

1.3. One-factorisations and Latin squares

There is a close relationship between Latin squares of order n and 1-factorisations of the complete bipartite graph $K_{n,n}$. Indeed, the correspondence is one-to-one if we insist that the Latin squares use disjoint sets Σ_1, Σ_2 and Σ_3 to index their rows, columns and symbols, respectively, that the two parts of $K_{n,n}$ are designated as first and second parts with vertices labelled by Σ_1 and Σ_2, respectively, and that the 1-factors are labelled by Σ_3. Each symbol in a square then gives rise to a set of n edges in $K_{n,n}$, according to the rule that if (r, c, s) is in the square, then this gives rise to the edge $\{r, c\}$. The Latin property ensures that the edges arising from each symbol form a 1-factor and that the 1-factors corresponding to distinct symbols are disjoint. Hence a Latin square of order n neatly encodes a 1-factorisation of $K_{n,n}$. Taking the union of two 1-factors in the 1-factorisation, we get (graphical) cycles in $K_{n,n}$ which correspond exactly to symbol cycles of the Latin square. In fact, it is easy to see that the 1-factorisation is perfect if and only if the corresponding Latin square is symbol-Hamiltonian.

Note that the roles of rows, columns and symbols can be permuted in the above discussion and this gives rise to several essentially equivalent formulations.

There is a well-known construction of a Latin square of order n (or equivalently, a 1-factorisation of the complete bipartite graph $K_{n,n}$) from a 1-factorisation of the complete graph K_{n+1}. Following [18], we call this the $\mathbb{K}$-construction. It appears to have been discovered independently by a number of different researchers. Laufer [10] and Keedwell [9] use it without accreditation and Dénes and Keedwell [6] attribute it to "Rosa and others".

We define a *rooted* 1*-factorisation* of a graph G with vertex set V to be a pair $(\mathcal{F}, v)$ where $\mathcal{F}$ is a 1-factorisation of G and $v \in V$. The vertex v will be called the *root*. From such a rooted 1-factorisation, the $\mathbb{K}$-construction produces a Latin square, which we denote by $\mathcal{L}(\mathcal{F}, v)$ and which has $\Sigma = V \setminus \{v\}$ as its index set. The Latin square is *idempotent*, meaning that it contains the triple (x, x, x) for each $x \in \Sigma$. For any distinct $x, y \in \Sigma$ the entry in row x, column y is defined to be the unique z for which $\{x, y\}$ and $\{v, z\}$ are edges

in the same 1-factor in $\mathcal{F}$. It is a simple matter to check that this does properly define a Latin square $\mathcal{L}(\mathcal{F}, v)$ and that this square is symmetric.

After constructing two 1-factorisations of K_{p+1} in Section 3, our focus will shift to the Latin squares produced by applying the $\mathbb{K}$-construction to our 1-factorisations. In Section 4 we find the full paratopy group of each of these Latin squares and in Section 5 we establish that the squares are atomic provided 2 is a primitive root modulo p. In the process, we discover two new families of atomic latin squares and show that the squares in one of these families have a trivial autotopy group.

While the $\mathbb{K}$-construction always produces a Latin square, it is certainly not true that every Latin square (or even a representative of every main class of Latin square) can be produced by the $\mathbb{K}$-construction. A cubic time algorithm is given in [18] for deciding whether a main class contains a symmetric idempotent square (in other words, a square constructible by the $\mathbb{K}$-construction). The same paper contains proofs of the following two results which we shall need later.

Theorem 1.3. *Let $(\mathcal{F}, u)$ and $(\mathcal{G}, v)$ be two rooted 1-factorisations of K_n. The following three statements are equivalent*:

(1) *$\mathcal{L}(\mathcal{F}, u)$ is paratopic to $\mathcal{L}(\mathcal{G}, v)$;*
(2) *$\mathcal{L}(\mathcal{F}, u)$ is isomorphic to $\mathcal{L}(\mathcal{G}, v)$;*
(3) *$\mathcal{F}$ is isomorphic to $\mathcal{G}$ by an isomorphism which maps u to v.*

Theorem 1.4. *Let $(\mathcal{F}, v)$ be a rooted 1-factorisation of K_{n+1}. Then $\mathcal{L}(\mathcal{F}, v)$ is symbol-Hamiltonian if and only if $\mathcal{F}$ is perfect.*

This second theorem is classical although it is often stated without the "only if" implication. Both the "if" and the "only if" implications will be crucial to our results in Section 5.

Theorem 1.3 shows the slightly surprising result that the $\mathbb{K}$-construction can produce different main classes (and hence non-isomorphic factorisations of $K_{n,n}$) merely by choosing a different root. This observation will help us to generate five interesting families of Latin squares in Section 4.

2. The folding operation

Let A be a symmetric Latin square of odd order n. It is well known that each of the n symbols of A occurs once on the main diagonal of A. Let x be any member of the index set of A. We now define an operation on A, which we call an *x-fold*. This operation will produce a new Latin square $A' = A'(x)$ which is identical to A except for entries which lie in row x, column x or the main diagonal. The entries on the main diagonal are switched with those in row x and column x. Formally, we define the x-fold of A by

$$A'_{i,j} = \begin{cases} A_{i,i} & \text{if } j = x, \\ A_{j,j} & \text{if } i = x, \\ A_{x,i} & \text{if } i = j, \\ A_{i,j} & \text{otherwise.} \end{cases}$$

The significance of this operation is demonstrated by our next lemma. We need the following definition. Let $\mathcal{F}$ be a 1-factorisation of the complete graph. We define $s_{\mathcal{F}}(b, \{c, d\}) = a$ if and only if $\{a, b\}$ and $\{c, d\}$ are in the same 1-factor of $\mathcal{F}$.

Lemma 2.1. *Let $\mathcal{F}$ be a 1-factorisation of a complete graph in which two distinct vertices are labelled u and v. If $A = \mathcal{L}(\mathcal{F}, u)$ and $B = \mathcal{L}(\mathcal{F}, v)$, then B is isotopic to the v-fold of A and A is isotopic to the u-fold of B.*

Proof. Let $A = \mathcal{L}(\mathcal{F}, u)$ and $B = \mathcal{L}(\mathcal{F}, v)$ and let A' be the v-fold of A. Also, let V be the set of vertices in $\mathcal{F}$. We define two bijections from the index set of A, namely $V \setminus \{u\}$, to the index set of B, namely $V \setminus \{v\}$. Let π be the bijection defined by $v \mapsto u$ and $i \mapsto i$ for $i \neq v$. Let τ be the bijection defined by $x \mapsto s_{\mathcal{F}}(v, \{u, x\})$ for all x. A simple consequence of this definition is that for arbitrary distinct vertices $x, y \in V$,

$$s_{\mathcal{F}}(u, \{x, y\}) \mapsto s_{\mathcal{F}}(v, \{x, y\})$$

under τ. Also $v \mapsto u$.

Let A'' be the Latin square obtained from A' by applying τ to the symbols and π to the row and column indices of A'. We show that A'' is equal to B, by considering an edge $\{x, y\}$ of the complete graph and determining which triples it gives rise to in A and B.

Case 1: $\{x, y\} = \{u, v\}$

Then $(v, v, v) \in A$ and $(u, u, u) \in B$. But the former implies that $(v, v, v) \in A'$, so $(u, u, u) \in A''$.

Case 2: $\{x, y\} = \{u, y\}$, $y \neq v$

Then $(y, y, y) \in A$ and $\big(u, y, s_{\mathcal{F}}(v, \{u, y\})\big) \in B$. But the former implies that $(v, y, y) \in A'$, so $\big(u, y, s_{\mathcal{F}}(v, \{u, y\})\big) \in A''$.

Case 3: $\{x, y\} = \{v, y\}$, $y \neq u$

Then $\big(v, y, s_{\mathcal{F}}(u, \{v, y\})\big) \in A$ and $(y, y, y) \in B$. But the former implies that $\big(y, y, s_{\mathcal{F}}(u, \{v, y\})\big) \in A'$, so $(y, y, y) \in A''$.

Case 4: $\{x, y\} \cap \{u, v\} = \emptyset$

Then $\big(x, y, s_{\mathcal{F}}(u, \{x, y\})\big) \in A$ and $\big(x, y, s_{\mathcal{F}}(v, \{x, y\})\big) \in B$. But the former implies that $\big(x, y, s_{\mathcal{F}}(u, \{x, y\})\big) \in A'$, so $\big(x, y, s_{\mathcal{F}}(v, \{x, y\})\big) \in A''$.

Thus $B = A''$ is isotopic to the v-fold of A and (by symmetry) A is isotopic to the u-fold of B. □

Note that the above result, together with Theorem 1.3, implies that folding will sometimes preserve the main class (when u is in the same orbit as v in the automorphism group of $\mathcal{F}$), but in other cases it will change the main class.

Importantly, as our next few results show, folding tends to preserve Hamiltonian cycles even when it does not preserve the main class.

Lemma 2.2. *Suppose k is any element of the index set of a symmetric symbol-Hamiltonian square A of odd order. If B is the k-fold of A, then B is symbol-Hamiltonian.*

Proof. Since A is symmetric and has odd order, say n, we can permute its symbols to obtain an idempotent symmetric Latin square C. Now $C = \mathcal{L}(F, v)$ for some rooted

1-factorisation (F, v) of K_{n+1} which has k as one of its vertices. By Lemma 2.1, the Latin square $D = \mathcal{L}(F, k)$ is isotopic to the k-fold of C and hence also to B, since the operations of folding and permuting symbols commute. The symbol-Hamiltonian property is preserved by isotopy, which together with Theorem 1.4 means that F is perfect and C, D and B are all symbol-Hamiltonian. □

We also have the following result for row cycles (and a corresponding result holds for column cycles, by symmetry).

Lemma 2.3. *Let i, j, k be three distinct elements of the index set of a symmetric Latin square A. If A has a Hamiltonian row cycle between rows i and j, then so does the k-fold of A.*

Proof. Since k is distinct from i and j, the only effect that the folding has on rows i and j is to replace the triples

$$(i, i, A_{i,i}),\ (j, j, A_{j,j}),\ (i, k, A_{i,k}), (j, k, A_{j,k})$$

with the triples

$$(i, i, A_{i,k}),\ (j, j, A_{j,k}),\ (i, k, A_{i,i}), (j, k, A_{j,j}).$$

Now A is assumed to be symmetric, so $A_{i,j} = A_{j,i}$. This means that $D\left(\sigma_{i,j}(A)\right)$ contains $A_{i,i} \to A_{i,j} \to A_{j,j}$ and $A_{i,k} \to A_{j,k}$ as subpaths. The k-fold replaces these with $A_{i,i} \to A_{j,j}$ and $A_{i,k} \to A_{i,j} \to A_{j,k}$. In other words, folding simply changes the position of $A_{i,j}$ in the cycle, and this does not change the length of the cycle. □

Corollary 2.1. *Let A be a row-Hamiltonian Latin square and let A' be the k-fold of A for some k. Then all row cycles in A' are Hamiltonian except possibly those involving row k.*

3. Two families of 1-factorisations

In this section we describe two even starter induced 1-factorisations of K_{p+1}, where $p \geqslant 11$ is a prime. Let the vertex set of K_{p+1} be $\mathbb{Z}_p^* \cup \{\infty_1, \infty_2\}$, where $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$. All calculations are performed in the field $\mathbb{Z}_p$ and we define $i\infty_1 = \infty_1 i = \infty_1$ and $i\infty_2 = \infty_2 i = \infty_2$ for all $i \in \mathbb{Z}_p^*$.

Define the first even starter E_A on the (multiplicative) group $\mathbb{Z}_p^*$ by

$$E_A = \left\{\{x, y\} : x, y \in \mathbb{Z}_p^* \setminus \{1, \tfrac{1}{2}\} \text{ and } x + y = 1\right\}.$$

We verify that E_A is an even starter with $m_{E_A} = \frac{1}{2}$ and $g^* = -1$. If $i \in \mathbb{Z}_p^* \setminus \{1, -1\}$, then $\{x, y\} \in E_A$ where $x = (1 + i)^{-1}$ and $y = 1 - (1 + i)^{-1} = i(1 + i)^{-1}$. Hence $x^{-1}y = i$, and so $i \in \left\{x^{-1}y, y^{-1}x : \{x, y\} \in E_A\right\}$. Conversely, if $i = x^{-1}y$ for some $\{x, y\} \in E_A$, then $i = x^{-1}(1 - x) = x^{-1} - 1$ for some $x \in \mathbb{Z}_p^* \setminus \{1, \frac{1}{2}\}$ and so $i \neq -1, 0, 1$ and we have $i \in \mathbb{Z}_p^* \setminus \{1, -1\}$.

Let $\mathcal{F}^A$ be the 1-factorisation of K_{p+1} induced by E_A. Thus $\mathcal{F}^A$ has 1-factors $F_1^A, F_2^A, \ldots, F_{p-1}^A, F_0^A$ where

$$F_i^A = \left\{\{ix, iy\} : \{x, y\} \in E_A\right\} \cup \left\{\{i, \infty_1\}, \{\tfrac{1}{2}i, \infty_2\}\right\} \quad \text{for } i \in \mathbb{Z}_p^*,$$
$$F_0^A = \left\{\{x, y\} : x, y \in \mathbb{Z}_p^* \text{ and } x + y = 0\right\} \cup \left\{\{\infty_1, \infty_2\}\right\}.$$

It is easy to see that $\mathcal{F}^A$ is isomorphic to the 1-factorisation GK_{p+1}. Given $\mathcal{F}^A$, simply relabel the vertex ∞_1 as 0, ∞_2 as ∞, and reorder the 1-factors.

We obtain the second even starter E_B from E_A by removing the pair $\{-1, 2\}$ and replacing it with $\{-1, \frac{1}{2}\}$. Thus we define E_B on the (multiplicative) group $\mathbb{Z}_p^*$ by

$$E_B = \left\{\{x, y\} : x, y \in \mathbb{Z}_p^* \setminus \{1, 2, \tfrac{1}{2}, -1\} \text{ and } x + y = 1\right\} \cup \left\{\{-1, \tfrac{1}{2}\}\right\}.$$

We verify that E_B is an even starter with $m_{E_B} = 2$ and $g^* = -1$. Since $\{-1, \frac{1}{2}\} \in E_B$ we have $-\frac{1}{2}, -2 \in \left\{x^{-1}y, y^{-1}x : \{x, y\} \in E_B\right\}$. If $i \in \mathbb{Z}_p^* \setminus \{1, -1, -\frac{1}{2}, -2\}$ then $\{x, y\} \in E_B$ where $x = (1 + i)^{-1}$ and $y = 1 - (1 + i)^{-1} = i(1 + i)^{-1}$. Hence $x^{-1}y = i$, and so $i \in \left\{x^{-1}y, y^{-1}x : \{x, y\} \in E_B\right\}$. Conversely, if $i = x^{-1}y$ for some $\{x, y\} \in E_B$, then $i = x^{-1}(1 - x) = x^{-1} - 1$ for some $x \in \mathbb{Z}_p^* \setminus \{1, 2, \frac{1}{2}, -1\}$ or $i \in \left\{-\frac{1}{2}, -2\right\}$ and we have $i \in \mathbb{Z}_p^* \setminus \{1, -1\}$.

Let $\mathcal{F}^B$ be the 1-factorisation of K_{p+1} induced by E_B. Thus $\mathcal{F}^B$ has 1-factors $F_1^B, F_2^B, \ldots, F_{p-1}^B, F_0^B$, where

$$F_i^B = \left\{\{ix, iy\} : \{x, y\} \in E_B\right\} \cup \left\{\{i, \infty_1\}, \{2i, \infty_2\}\right\} \quad \text{for } i \in \mathbb{Z}_p^*,$$
$$F_0^B = \left\{\{x, y\} : x, y \in \mathbb{Z}_p^* \text{ and } x + y = 0\right\} \cup \left\{\{\infty_1, \infty_2\}\right\}.$$

We will use an invariant called a *train* to show that $\mathcal{F}^A$ and $\mathcal{F}^B$ are not isomorphic. Trains were first introduced by White [19], and have been used to distinguish Steiner triple systems [5], 1-factorisations [7] and Latin squares [17].

Suppose $\mathcal{F}$ is a 1-factorisation of K_{2n}. The *train* of $\mathcal{F}$ is a directed graph whose vertices are the $n(2n-1)^2$ triples $(\{x, y\}, F)$, where $\{x, y\}$ is an unordered pair of distinct vertices of K_{2n} and F is a factor in $\mathcal{F}$. There is a directed edge from $(\{x, y\}, F)$ to $(\{w, z\}, G)$ in the train of $\mathcal{F}$ if and only if

- $\{x, y\}$ is an edge in G;
- $\{x, z\}$ is an edge in F;
- $\{y, w\}$ is an edge in F.

It is clear that each vertex of a train has out-degree 1 and that isomorphic 1-factorisations have isomorphic trains.

Lemma 3.1. *The 1-factorisations $\mathcal{F}^A$ and $\mathcal{F}^B$ are not isomorphic.*

Proof. It was shown in [7] that, for all odd primes p, the train of $\mathcal{F}^A$ has maximum in-degree two. We now show that $d = \left(\{\frac{1}{2}, -\frac{7}{4}\}, 1\right)$ has in-degree at least three in the train of $\mathcal{F}^B$, thus showing that $\mathcal{F}^A$ and $\mathcal{F}^B$ are not isomorphic.

We first treat the case $p \neq 13$.

By definition, F_1^B contains $\{-1, \frac{1}{2}\}$ and $\{2, \infty_2\}$. For $p \neq 13$, it is straightforward to check that the (not necessarily distinct) edges

$$\{\tfrac{13}{8}, -\tfrac{5}{8}\}, \{-13, 14\}, \{5, -4\}, \{8, -7\}, \{-\tfrac{1}{4}, \tfrac{5}{4}\} \text{ and } \{-\tfrac{5}{2}, \tfrac{7}{2}\}$$

are also in F_1^B since each edge $\{x, y\}$ in the above list satisfies $x + y = 1$ and $\{x, y\} \cap \{0, \frac{1}{2}, -1, 2\} = \emptyset$.

We now show that in the train of $\mathcal{F}^B$ there is a directed edge from each of the vertices

$$a = \left(\{\tfrac{13}{8}, -\tfrac{5}{8}\}, -\tfrac{1}{8}\right), \quad b = \left(\{2, \infty_2\}, \tfrac{1}{4}\right) \quad \text{and} \quad c = \left(\{-\tfrac{1}{4}, \tfrac{5}{4}\}, -\tfrac{1}{2}\right)$$

to the vertex d. Notice that a, b, c and d are distinct vertices for $p \geqslant 11$.

Since $\{-13, 14\}, \{5, -4\} \in F_1^B$, we have $\{\frac{13}{8}, -\frac{7}{4}\}, \{-\frac{5}{8}, \frac{1}{2}\} \in F_{-1/8}^B$ and so since $\{\frac{13}{8}, -\frac{5}{8}\} \in F_1^B$, there is a directed edge from a to d.

Since $\{2, \infty_2\}, \{8, -7\} \in F_1^B$, we have $\{\frac{1}{2}, \infty_2\}, \{2, -\frac{7}{4}\} \in F_{1/4}^B$ and so there is a directed edge from b to d.

Finally, since $\{-\frac{5}{2}, \frac{7}{2}\}, \{-1, \frac{1}{2}\} \in F_1^B$, we have $\{\frac{5}{4}, -\frac{7}{4}\}, \{\frac{1}{2}, -\frac{1}{4}\} \in F_{-1/2}^B$ and so since $\{-\frac{1}{4}, \frac{5}{4}\} \in F_1^B$, there is a directed edge from c to d.

It is easy to check that when $p = 13$ there are directed edges from a', b and c to d, where $a' = \left(\{\infty_1, -\frac{5}{8}\}, -\frac{1}{8}\right)$. □

We now investigate the automorphism groups of $\mathcal{F}^A$ and $\mathcal{F}^B$. To do this we make use of a theorem due to Ihrig [8, Theorem 5.10].

Theorem 3.1. *Let $\mathcal{F}$ be an even starter induced 1-factorisation of K_{p+1}. If $\mathcal{F}$ is not isomorphic to GK_{p+1}, then the automorphism group of $\mathcal{F}$ is the starter group.*

It is clear for $i \in \mathbb{Z}_p^*$ that $\pi_i(x) = xi$ is an automorphism of both $\mathcal{F}^A$ and $\mathcal{F}^B$. Since $\mathcal{F}^B$ is an even starter induced 1-factorisation of K_{p+1}, it follows from Theorem 3.1 and Lemma 3.1 that it can have no other automorphisms. Hence $|\mathrm{Aut}(\mathcal{F}^B)| = p - 1$ and $\mathrm{Aut}(\mathcal{F}^B)$ has three orbits, namely, $\mathbb{Z}_p^*$, $\{\infty_1\}$ and $\{\infty_2\}$.

The automorphisms of $\mathcal{F}^A$ were discussed in the context of GK_{p+1} in Section 1.1. From there we deduce that $|\mathrm{Aut}(\mathcal{F}^A)| = p(p-1)$ and that $\mathcal{F}^A$ has a cyclic automorphism ρ defined by

$$\rho(x) = \begin{cases} 1 & \text{if } x = \infty_1, \\ \infty_1 & \text{if } x = p - 1, \\ x + 1 & \text{otherwise.} \end{cases}$$

Together with the automorphisms π_i given above, ρ generates $\mathrm{Aut}(\mathcal{F}^A)$, which therefore has two orbits, $\mathbb{Z}_p^* \cup \{\infty_1\}$ and $\{\infty_2\}$.

4. Five families of Latin squares

We now describe five main classes of Latin square which, for any given prime $p \geqslant 11$, can be obtained from $\mathcal{F}^A$ and $\mathcal{F}^B$ using the $\mathbb{K}$-construction. For each of our Latin squares we will use $\mathbb{Z}_p$ as the index set, although this may require some relabelling after applying the $\mathbb{K}$-construction.

Since the automorphism group of $\mathcal{F}^A$ has two orbits, Theorem 1.3 tells us that applying the $\mathbb{K}$-construction to $\mathcal{F}^A$ gives rise to two main classes of Latin square. Let $\mathcal{M}_1$ be the main class of Latin squares obtained by choosing ∞_2 as the root. Let $\mathcal{M}_2$ be the main class of Latin squares obtained by choosing an element of $\mathbb{Z}_p^* \cup \{\infty_1\}$ as the root.

We define $L_1 \in \mathcal{M}_1$ to be the Latin square obtained from $\mathcal{F}^A$ by choosing ∞_2 as the root in the $\mathbb{K}$-construction and labelling ∞_1 as 0. Hence L_1 is described by the triples

$$\left(i, j, \tfrac{1}{2}(i+j)\right) \quad \text{for } i, j \in \mathbb{Z}_p.$$

We define $L_2 \in \mathcal{M}_2$ to be the Latin square obtained from $\mathcal{F}^A$ by choosing ∞_1 as the root in the $\mathbb{K}$-construction and labelling ∞_2 as 0. Hence, L_2 is described by the triples

$$\begin{cases} (i,i,i) & \text{for } i \in \mathbb{Z}_p, \\ (i,0,2i) & \text{for } i \in \mathbb{Z}_p^*, \\ (0,j,2j) & \text{for } j \in \mathbb{Z}_p^*, \\ (i,j,i+j) & \text{otherwise.} \end{cases}$$

Since the automorphism group of $\mathcal{F}^B$ has three orbits, Theorem 1.3 tells us that applying the $\mathbb{K}$-construction to $\mathcal{F}^B$ gives rise to three main classes of Latin square. Let $\mathcal{M}_3$, $\mathcal{M}_4$ and $\mathcal{M}_5$ be the main classes obtained by choosing, respectively, ∞_2, ∞_1 and an element of $\mathbb{Z}_p^*$ as the root.

We define $L_3 \in \mathcal{M}_3$ to be the square obtained from $\mathcal{F}^B$ by choosing ∞_2 as the root in the $\mathbb{K}$-construction and labelling ∞_1 as 0. Hence, L_3 is described by the triples

$$\begin{cases} (i,i,i) & \text{for } i \in \mathbb{Z}_p, \\ (i,-\frac{1}{2}i,-2i) & \text{for } i \in \mathbb{Z}_p^*, \\ (-\frac{1}{2}i,i,-2i) & \text{for } i \in \mathbb{Z}_p^*, \\ (i,j,2i+2j) & \text{otherwise.} \end{cases}$$

We define $L_4 \in \mathcal{M}_4$ to be the square obtained from $\mathcal{F}^B$ by choosing ∞_1 as the root in the $\mathbb{K}$-construction and labelling ∞_2 as 0. Hence, L_4 is described by the triples

$$\begin{cases} (i,i,i) & \text{for } i \in \mathbb{Z}_p, \\ (i,0,\frac{1}{2}i) & \text{for } i \in \mathbb{Z}_p^*, \\ (0,j,\frac{1}{2}j) & \text{for } j \in \mathbb{Z}_p^*, \\ (-i,\frac{1}{2}i,i) & \text{for } i \in \mathbb{Z}_p^*, \\ (\frac{1}{2}i,-i,i) & \text{for } i \in \mathbb{Z}_p^*, \\ (i,j,i+j) & \text{otherwise.} \end{cases}$$

We define $L_5 \in \mathcal{M}_5$ to be the square obtained from $\mathcal{F}^B$ by choosing 1 as the root in the $\mathbb{K}$-construction, and labelling ∞_1 as 0 and ∞_2 as 1. The description of the triples of L_5 is somewhat complicated. However, let L_5' be the symmetric Latin square described by the triples:

$$\begin{cases} (1, i, i) & \text{for } i \in \mathbb{Z}_p, \\ (i, 1, i) & \text{for } i \in \mathbb{Z}_p, \\ (i, i, 2i+2) & \text{for } i \in \mathbb{Z}_p \setminus \{1, -\frac{1}{2}, -2\}, \\ (-2, -2, 4) & \\ (i, -\frac{1}{2}i, -2i) & \text{for } i \in \mathbb{Z}_p \setminus \{0, 1, -2\}, \\ (-\frac{1}{2}i, i, -2i) & \text{for } i \in \mathbb{Z}_p \setminus \{0, 1, -2\}, \\ (i, j, 2i+2j) & \text{otherwise.} \end{cases}$$

It is easily verified that L_5' is the 1-fold of L_3. Hence by Lemma 2.1, L_5' is isotopic to L_5. We will use L_5' as our representative of $\mathcal{M}_5$ in later calculations.

Consider the two main classes of Latin squares arising from $\mathcal{F}^A$. Since $(i, j, k) \in L_1$ if and only if $i + j = 2k \bmod p$, we see that L_1 is isotopic to the Cayley table for the additive group $\mathbb{Z}_p$. Thus, $\mathcal{M}_1$ is a well-known class of Latin squares. Since $\mathcal{F}^A$ gives rise to only two main classes of Latin square, $\mathcal{M}_2$ must contain the squares described by Wanless [15], who studied the Latin squares which are not in the main class of the cyclic group but come from the same 1-factorisation of K_{p+1}. These squares had earlier been studied by Yamamoto (see Section 5).

Now consider the three main classes of Latin squares arising from $\mathcal{F}^B$. The square L_3 is isotopic to the square described by Owens and Preece [12]. If we multiply each symbol in L_3 by $\frac{1}{2}$, then we obtain exactly the square described in [12]. As far as we are aware, $\mathcal{M}_4$ and $\mathcal{M}_5$ have not been previously described in the literature except for the case $p = 11$ which was studied in [11].

We next state a theorem from [18] which will enable us to find the autotopy groups of each of our five main classes.

Theorem 4.1. *Let $L = \mathcal{L}(\mathcal{F}, v)$ for some rooted 1-factorisation $(\mathcal{F}, v)$ of K_{p+1} where p is prime. The automorphism group of L is isomorphic to the stabiliser of v in the automorphism group of $\mathcal{F}$. Moreover, every autotopy of L is an automorphism of L unless L is isotopic to the Cayley table of $\mathbb{Z}_p$.*

Let Λ be the group of isomorphisms each of which applies the permutation $x \mapsto \lambda x$ simultaneously to the row, column and symbol indices of a Latin square, for some $\lambda \in \mathbb{Z}_p^*$. Note that Λ is isomorphic to $\mathbb{Z}_{p-1}$.

The automorphism groups of $\mathcal{F}^A$ and $\mathcal{F}^B$ were identified in the previous section. Employing Theorem 4.1 immediately reveals that squares in $\mathcal{M}_5$ have trivial autotopy group while the autotopy group of L_2, L_3 and L_4 in each case is exactly Λ. In particular, L_2, L_3 and L_4 are of B_1-type. Also, Λ is a subset of the autotopies of L_1 (which is simultaneously of B_0-type and B_1-type). This helps to explain the observation in [11] that four of the seven main classes of atomic Latin squares of order 11 contain strikingly similar B_1-type squares.

The autotopy group of the Cayley table of $\mathbb{Z}_p$ (and hence also, the autotopy group of L_1) is well known and has order $p^2(p-1)$. See, for example, [11].

We have identified all autotopies of our Latin squares. Our next goal is to identify the autoparatopies. To do this we first diagnose which of our main classes contain totally symmetric squares.

It is well known that $\mathcal{M}_1$ contains a totally symmetric square. In fact, the Cayley table of any abelian group is isotopic to a totally symmetric square defined by $L_{i,j} = -i - j$ where i, j are arbitrary group elements.

Owens and Preece [12] showed that $\mathcal{M}_3$ consists of a single isotopy class. We next prove a stronger statement.

Lemma 4.1. *There is a totally symmetric B_1-type Latin square in $\mathcal{M}_3$.*

Proof. Let L_3' be the symmetric Latin square obtained by applying the permutation $x \to -\frac{1}{2}x$ to the symbols of L_3. We claim that L_3' is totally symmetric and of B_1-type. Let Λ denote the automorphism group of L_3 identified above. The isotopy which generates L_3' from L_3 commutes with every element of Λ, from which we infer that Λ is a subset of the automorphism group of L_3'. That is, L_3' is of B_1-type.

For a symmetric Latin square to be totally symmetric it is necessary and sufficient that it be involutory. To prove that L_3' is involutory it suffices, by [16, Theorem 13], to show that $\sigma_1(L_3')$ is an involution. This is clear since by construction, row 1 of L_3' is given by the triples

$$(1, 1, -\tfrac{1}{2}), (1, -\tfrac{1}{2}, 1), (1, -2, -2) \quad \text{and}$$

$$(1, j, -1-j) \quad \text{for} \quad j \in \mathbb{Z}_p \setminus \{1, -\tfrac{1}{2}, -2\}. \qquad \square$$

It turns out that the three remaining main classes do not contain totally symmetric squares. To prove this we will use the following result from [18].

Lemma 4.2. *The main class of a symmetric Latin square L contains a totally symmetric square if and only if there is some permutation which, when applied to the symbols of L, produces a totally symmetric square.*

Lemma 4.3. *There is no totally symmetric Latin square in $\mathcal{M}_2$ or $\mathcal{M}_4$.*

Proof. Let L be either L_2 or L_4. Employing Lemma 4.2, we assume that there exists a symbol permutation τ that takes L to a totally symmetric square M. First suppose that $\tau(0) = x \neq 0$. Let

$$i \in \mathbb{Z}_p \setminus \{0,\ -x,\ x,\ -2x,\ -\tfrac{1}{2}x\}.$$

As $p \geqslant 11$ it is clear that we have at least six distinct choices for such an i.

Now by the definition of L and i we know that L contains the triples $(i, -i, 0)$, $(i, x, i+x)$, $(i+x, i+x, i+x)$ and $(i+x, -i, x)$. The first of these implies that $(i, -i, x) \in M$ and hence, by total symmetry, $(i, x, -i) \in M$. This means that $\tau(i+x) = -i$ and hence

$(i+x, i+x, -i) \in M$ and, by total symmetry, $(i+x, -i, i+x) \in M$. But this tells us that $\tau(x) = i + x$ which cannot be true simultaneously for the distinct values of i.

That leaves the case $\tau(0) = 0$. For any $i \in \mathbb{Z}_p$ we know that L has triples $(i, -i, 0)$ and (i, i, i). From the first of these we infer that $(i, -i, 0) \in M$ and $(i, 0, -i) \in M$.

We now split this into two subcases. First, suppose that $L = L_2$. Here, $(i, 0, 2i) \in L$ for all $i \in \mathbb{Z}_p$ so that $\tau(2i) = -i$ and M contains the triples $(i, i, -\frac{1}{2}i)$ and $(i, -\frac{1}{2}i, i)$. But L_2 contains $(i, -\frac{1}{2}i, \frac{1}{2}i)$ for all $i \in \mathbb{Z}_p$ which implies that $\tau(\frac{1}{2}i) = i$. Our two rules for τ are incompatible, for example they imply that $-1 = \tau(2) = 4$.

The subcase $L = L_4$ works similarly. Here, $(i, 0, \frac{1}{2}i) \in L$ so $\tau(\frac{1}{2}i) = -i$ for all $i \in \mathbb{Z}_p$ and M contains the triples $(i, i, -2i)$ and $(i, -2i, i)$. But L_4 contains $(i, -2i, 2i)$ which implies that $\tau(2i) = i$ for all $i \in \mathbb{Z}_p$. This gives the contradiction $1 = \tau(2) = -4$.

We conclude that M cannot exist. □

Lemma 4.4. *There is no totally symmetric Latin square in $\mathcal{M}_5$.*

Proof. As before, we assume that there exists a symbol permutation τ that takes L_5' to a totally symmetric square M. First, suppose that $\tau(0) = x \neq 1$. Let

$$i \in \mathbb{Z}_p \setminus \{0,\ 1,\ -1,\ x,\ -2x,\ -\tfrac{1}{2}x,\ 2-x,\ \tfrac{1}{2}-x,\ -1-x,\ x-1,\ 2-2x,\ \tfrac{1}{2}-\tfrac{1}{2}x\}.$$

For $p > 13$ it is clear that we have at least two distinct choices for such an i. This is also true for $p \in \{11, 13\}$ as can easily be checked for each value of $x \in \mathbb{Z}_p \setminus \{1\}$ by computing the above set.

Now by the definition of L_5' and i, we know that L_5' contains the triples $(i, -i, 0)$, $(i, x, 2i + 2x)$, $(i + x - 1, i + x - 1, 2i + 2x)$ and $(i + x - 1, -i, 2x - 2)$. The first of these implies that $(i, -i, x) \in M$ and hence, by total symmetry, $(i, x, -i) \in M$. This means that $\tau(2i + 2x) = -i$, which in turn means that $(i + x - 1, i + x - 1, -i) \in M$. By total symmetry we then infer that $(i + x - 1, -i, i + x - 1) \in M$. But this implies $\tau(2x - 2) = i + x - 1$ which cannot be true simultaneously for two distinct values of i.

That leaves the case $\tau(0) = 1$. As $p \geqslant 11$, we can choose

$$i \in \mathbb{Z}_p \setminus \{0,\ 1,\ -1,\ -2,\ 4,\ -3,\ \tfrac{2}{3},\ -\tfrac{2}{3},\ -6\}.$$

The choice of i ensures that L_5' contains the triples $(i, -i, 0)$, $(i, 1, i)$, $(-i - 2, i + 2, 0)$, $(-i-2, 1, -i-2)$, $(\frac{1}{2}i-1, \frac{1}{2}i-1, i)$ and $(\frac{1}{2}i-1, -i, -i-2)$. We deduce that M contains $(i, -i, 1)$ and $(-i-2, i+2, 1)$, and by total symmetry also $(i, 1, -i)$ and $(-i-2, 1, i+2)$. Thus $\tau(i) = -i$ and $\tau(-i - 2) = i + 2$. Hence $(\frac{1}{2}i - 1, \frac{1}{2}i - 1, -i) \in M$ and by total symmetry $(\frac{1}{2}i - 1, -i, \frac{1}{2}i - 1) \in M$. But this means that $\tau(-i - 2) = \frac{1}{2}i - 1$. Thus $i + 2 = \frac{1}{2}i - 1$ and we find that $i = -6$ in contradiction of our choice of i. We conclude that M does not exist. □

Theorem 4.2. *Each of $\mathcal{M}_1$ and $\mathcal{M}_3$ consists of a single isotopy class. Each of $\mathcal{M}_2$, $\mathcal{M}_4$ and $\mathcal{M}_5$ consists of three distinct isotopy classes.*

Proof. By construction $L_i \in \mathcal{M}_i$ is symmetric for $i = 1, 2, \ldots, 5$, so each $\mathcal{M}_i$ consists of either 1 or 3 isotopy classes. By a theorem from [18], the main class of a symmetric Latin square consists of a single isotopy class if and only if the main class contains a totally symmetric square. The current result then follows immediately from its predecessors. □

We can now summarise the results of this section in table form. In the following table, for each main class, we give the order of the autotopy group, the order of the autoparatopy group and the number of Latin squares in the main class. This last number is $6p!^3$ divided by the order of the autoparatopy group.

Main class	Autotopies	Autoparatopies	Number of LS
$\mathcal{M}_1$	$p^2(p-1)$	$6p^2(p-1)$	$p!(p-1)!(p-2)!$
$\mathcal{M}_2$	$p-1$	$2(p-1)$	$3p!^2(p-2)!\,p$
$\mathcal{M}_3$	$p-1$	$6(p-1)$	$p!^2(p-2)!\,p$
$\mathcal{M}_4$	$p-1$	$2(p-1)$	$3p!^2(p-2)!\,p$
$\mathcal{M}_5$	1	2	$3p!^3$

5. Perfection and atomicity

In this section we investigate the related questions of whether the 1-factorisations we have described are perfect and whether our Latin squares are atomic.

Before achieving that goal, we first define a family of digraphs which will be useful in subsequent proofs. For any $c \in \mathbb{Z}_p$ let $D_{p,c} = D(\pi_{p,c})$ where $\pi_{p,c}$ is the permutation of $\mathbb{Z}_p$ defined by the rule $x \mapsto 2x + c$. Clearly, $D_{p,c}$ consists of a number of directed cycles, including a loop on the vertex $-c$. The number of cycles depends on $O(2, p)$, the order of 2 modulo p. Consider the cycle which contains the vertex $v \neq -c$. By induction, the kth vertex of this cycle (starting with v as the 0th vertex) is $2^k v + (2^k - 1)c$. Thus the cycle returns to v when $2^k v + (2^k - 1)c = v$, which is equivalent to $(2^k - 1)(v + c) = 0$. From this it is clear that aside from the loop on $-c$, every cycle in $D_{p,c}$ has length $O(2, p)$. In particular, when $O(2, p) = p - 1$ (that is, 2 is primitive), $D_{p,c}$ consists of a loop and just one other cycle, whereas if $O(2, p) < p - 1$ then $D_{p,c}$ consists of a loop and at least two other cycles.

It is well known that squares in $\mathcal{M}_1$ are atomic (assuming that p is prime). It was proved by Wanless [15] that the squares in $\mathcal{M}_2$ are atomic if and only if 2 is primitive modulo p. It seems that the same result was obtained much earlier by Yamamoto. In [20] he asserts that, in our terminology, a Latin square obtained by folding the Cayley table of the cyclic group of prime order p is not isotopic to that Cayley table but is nonetheless atomic if 2 is primitive modulo p. We are unaware of Yamamoto ever publishing a proof of his assertion.

It was shown in [12] that squares in $\mathcal{M}_3$ are atomic. We next use this fact to prove results for $\mathcal{M}_4$ and $\mathcal{M}_5$ which are analogous to the just mentioned result for $\mathcal{M}_2$.

Note that since L_3 is symbol-Hamiltonian it follows from Theorem 1.4 that $\mathcal{F}^B$ is perfect and that both L_4 and L_5 are symbol-Hamiltonian. The observation that $\mathcal{F}^B$ is perfect, together with Lemma 3.1, completes the proof of Theorem 1.1. As both L_4 and L_5 are symmetric and symbol-Hamiltonian, it follows that they are atomic if and only if they are row-Hamiltonian.

Theorem 5.1. *The squares in $\mathcal{M}_4$ are atomic if and only if 2 is primitive modulo p.*

Proof. Let L'_4 be the 0-fold of L_3. Note that $L'_4 \in \mathcal{M}_4$ by Lemma 2.1. Also, by Corollary 2.1 it suffices to consider row cycles involving row 0. Since L'_4 is obtained from L_4 by permuting the symbols, and L_4 has an automorphism which cyclically permutes the rows other than row 0, we see that L'_4 is atomic if and only if $\sigma_{0,1}(L_4)$ is a full cycle permutation.

Provided $j \notin \{0, 1, -\frac{1}{2}, -2\}$ then in column j of L_4 the entry in row 0 is $\frac{1}{2}j$ and the entry in row 1 is $j+1$. So, with a few exceptions, $\sigma_{0,1}(L_4)$ maps x to $2x+1$. Thus $D\left(\sigma_{0,1}(L_4)\right)$ can be obtained by a simple modification of $D_{p,1}$. In the case when $O(2, p) = p-1$, the cycle of length $p-1$ in $D_{p,1}$ contains subpaths $0 \to 1$ and $-\frac{1}{4} \to \frac{1}{2} \to 2$. According to the definition of L_4 we can obtain $D\left(\sigma_{0,1}(L_4)\right)$ from $D_{p,1}$ by replacing these paths with $0 \to \frac{1}{2} \to 1$ and $-\frac{1}{4} \to -1 \to 2$, and removing the loop on -1. This modification is illustrated in Fig. 1, from which it is clear that a Hamiltonian cycle is produced.

When $O(2, p) < p-1$ there are at least three cycles (counting the loop) in $D_{p,1}$ and the modification is the same: we replace $\frac{1}{2}$ with -1, insert $\frac{1}{2}$ between 0 and 1, and remove the loop. This modification decreases the number of cycles by 1, by eliminating the loop. Thus there are at least two cycles remaining, and the square is not atomic in this case. □

We now prove a similar result for $\mathcal{M}_5$. We use the Latin square L'_5 defined in Section 4. Recall that L'_5 is isotopic to L_5.

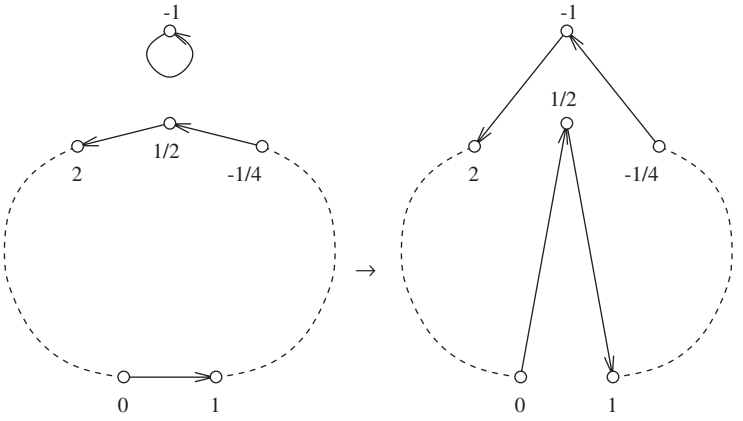

Fig. 1. Modification of $D_{p,1}$ to obtain $D\left(\sigma_{0,1}(L_4)\right)$.

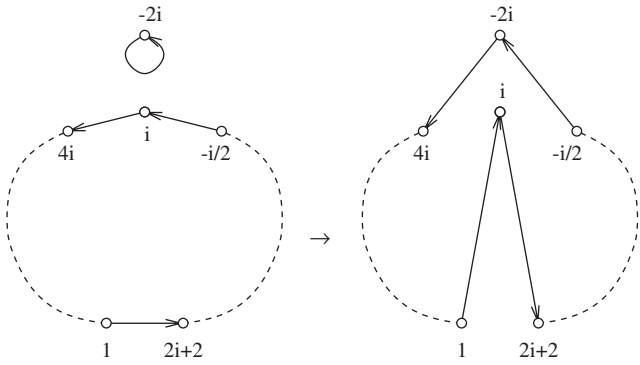

Fig. 2. Modification of $D_{p,2i}$ to obtain $D\left(\sigma_i(L'_5)\right)$.

Theorem 5.2. *The squares in $\mathcal{M}_5$ are atomic if and only if 2 is primitive modulo p.*

Proof. By Corollary 2.1, to establish whether L'_5 is atomic it suffices to consider row cycles involving row 1. Such cycles are easy to analyse, since $\sigma_1(L'_5)$ is the identity, so that $\sigma_{1,i}(L'_5) = \sigma_i(L'_5)$ for each i. Note that, with some exceptions, $\sigma_i(L'_5)$ typically maps x to $2x + 2i$ and hence $D\left(\sigma_i(L'_5)\right)$ can easily be obtained by modifying $D_{p,2i}$.

We first treat the case when $i = 0$. For $j \in \mathbb{Z}_p \setminus \{0, 1\}$ the entry in column j of row 0 is $2j$. Also note that $(0, 1, 0)$ and $(0, 0, 2)$ are triples of L'_5. Hence $D\left(\sigma_0(L'_5)\right)$ can be obtained from $D_{p,0}$ by removing the loop on 0 and the arc $1 \to 2$ and replacing them with the path $1 \to 0 \to 2$.

Secondly, we consider the case when $i = -\frac{1}{2}$. Since $(-\frac{1}{2}, \frac{1}{4}, 1)$ and $(-\frac{1}{2}, 1, -2)$ are triples of L'_5, $D\left(\sigma_{-1/2}(L'_5)\right)$ can be obtained from $D_{p,-1}$ by removing the loop on 1 and the arc $\frac{1}{4} \to -\frac{1}{2}$ and replacing them with the path $\frac{1}{4} \to 1 \to -\frac{1}{2}$.

Thirdly, we consider the case when $i = -2$. Since $(-2, 1, -2)$ and $(-2, -2, 4)$ are triples of L'_5, $D\left(\sigma_{-2}(L'_5)\right)$ can be obtained from $D_{p,-4}$ by removing the loop on 4 and the arc $-2 \to -8$ and replacing them with the path $-2 \to 4 \to -8$.

In the three cases considered so far it is clear that the modification produces a cycle of length $O(2, p) + 1$ and that any remaining cycles will have length $O(2, p)$. In particular, we get a Hamiltonian cycle if and only if 2 is primitive modulo p.

Finally, we consider the case when $i \in \mathbb{Z}_p \setminus \{0, 1, -\frac{1}{2}, -2\}$. According to the definition of L'_5 we can obtain $D\left(\sigma_i(L'_5)\right)$ from $D_{p,2i}$ by removing the loop on $-2i$ and the paths $1 \to 2i + 2$ and $-\frac{1}{2}i \to i \to 4i$ and replacing them with the paths $1 \to i \to 2i + 2$ and $-\frac{1}{2}i \to -2i \to 4i$. If 2 is primitive then this modification produces a Hamiltonian cycle, as illustrated in Fig. 2. □

6. Summary

Let $p \geqslant 11$ be a given prime. We have constructed an even starter induced 1-factorisation $\mathcal{F}^B$ of K_{p+1} which is not isomorphic (Lemma 3.1) to the patterned 1-factorisation $\mathcal{F}^A$, but which nonetheless is perfect (Section 5).

By applying the $\mathbb{K}$-construction to $\mathcal{F}^A$ and $\mathcal{F}^B$ we have constructed five main classes $\mathcal{M}_1$, $\mathcal{M}_2$, $\mathcal{M}_3$, $\mathcal{M}_4$ and $\mathcal{M}_5$ of Latin squares of order p. The first three of these were previously known, while the last two appear to be new. The squares in $\mathcal{M}_1$ and $\mathcal{M}_3$ are always atomic, whilst the squares in $\mathcal{M}_2$, $\mathcal{M}_4$ and $\mathcal{M}_5$ are atomic if and only if 2 is a primitive root modulo p (Theorems 5.1 and 5.2).

Both $\mathcal{M}_1$ and $\mathcal{M}_3$ contain totally symmetric squares (Theorem 4.1) and hence consist of a single isotopy class of atomic Latin squares. Each of these isotopy classes is equivalent to a perfect 1-factorisation of $K_{p,p}$. Each of $\mathcal{M}_2$, $\mathcal{M}_4$ and $\mathcal{M}_5$ contains three distinct isotopy classes (Theorem 4.2). When 2 is not a primitive root modulo p, only one of the three isotopy classes in each main class is symbol-Hamiltonian. Hence each of $\mathcal{M}_2$, $\mathcal{M}_4$ and $\mathcal{M}_5$ gives rise to either three (if 2 is primitive mod p) or one (for other primes) perfect 1-factorisations of $K_{p,p}$.

Hence, if 2 is primitive modulo p then we have constructed 11 non-isomorphic perfect 1-factorisations of $K_{p,p}$, while for other primes we have constructed five non-isomorphic perfect 1-factorisations of $K_{p,p}$.

References

[1] B.A. Anderson, Sequencings and starters, Pacific J. Math. 64 (1976) 17–24.
[2] B.A. Anderson, Symmetry groups of some perfect 1-factorizations of complete graphs, Discrete Math. 18 (1977) 227–234.
[3] D. Bryant, M. Buchanan, I.M. Wanless, The spectrum for quasigroups with cyclic automorphisms and additional symmetries, submitted for publication.
[4] D. Bryant, B.M. Maenhaut, I.M. Wanless, A family of perfect factorisations of complete bipartite graphs, J. Combin. Theory Ser. A 98 (2002) 328–342.
[5] M.J. Colbourn, C.J. Colbourn, W.L. Rosenbaum, Trains: an invariant for Steiner triple systems, Ars Combin. 13 (1982) 149–162.
[6] J. Dénes, A.D. Keedwell, Latin squares: new developments in the theory and applications, Ann. Discrete Math. 46 (1991).
[7] J.H. Dinitz, W.D. Wallis, Trains: an invariant for one-factorizations, Ars Combin. 32 (1991) 161–180.
[8] E.C. Ihrig, Symmetry groups related to the construction of perfect one factorizations of K_{2n}, J. Combin. Theory Ser. B 40 (1986) 121–151.
[9] A.D. Keedwell, Uniform P-circuit designs, quasigroups and room squares, Utilitas Math. 14 (1978) 141–159.
[10] P.J. Laufer, On strongly Hamiltonian complete bipartite graphs, Ars Combin. 9 (1980) 43–46.
[11] B.M. Maenhaut, I.M. Wanless, Atomic Latin squares of order eleven, J. Combin. Des. 12 (2004) 12–34.
[12] P.J. Owens, D.A. Preece, Some new non-cyclic Latin squares that have cyclic and Youden properties, Ars Combin. 44 (1996) 137–148.
[13] E. Seah, Perfect one-factorizations of the complete graph—a survey, Bull. Inst. Combin. Appl. 1 (1991) 59–70.
[14] W.D. Wallis, One-factorizations, Math. Appl. 390 (1997).
[15] I.M. Wanless, Perfect factorisations of complete bipartite graphs and Latin squares without proper subrectangles, Electron. J. Combin. 6 (1999) R9.
[16] I.M. Wanless, Diagonally cyclic Latin squares, European J. Combin. 25 (2004) 393–413.
[17] I.M. Wanless, Atomic Latin squares based on cyclotomic orthomorphisms, Electron. J. Combin. 12 (2005) R22.
[18] I.M. Wanless, E.C. Ihrig, Symmetries that Latin squares inherit from 1-factorizations, J. Combin. Designs 13 (2005) 157–172.
[19] M.S. White, Triple systems as transformations and their paths along triads, Trans. Amer. Math. Soc. 14 (1913) 6–13.
[20] K. Yamamoto, Generation principles of Latin squares, Bull. Inst. Internat. Statist. 38 (1961) 73–76.